55. Online Safety Policy

EYFS: 3.4-3.7

Our nursery is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers and strives to support children, staff and families in using the internet safely.

We refer to *'Safeguarding children and protecting professionals in early years settings: online safety considerations'* to support this policy.

Keeping Children Safe in Education states *"The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:*

- ✓ *content: being exposed to illegal, inappropriate or harmful material;*
- ✓ *contact: being subjected to harmful online interaction with other users; and*
- ✓ *conduct: personal online behaviour that increases the likelihood of, or causes,*
  harm."

The Designated Safeguarding Lead is ultimately responsible for online safety concerns. All concerns need to be raised as soon as possible to Carol Daly or Jodie Hursthouse, Designated Safeguarding Leads, or the Deputy Designated Safeguarding Leads, Seren Brown and Chelsea Dakin

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation: technology often provides the platform that facilitates harm.

The breadth of issues included within online safety is considerable but can be categorised into three areas of risk.

Content: Being exposed to illegal, inappropriate or harmful material, for example pornography, fake news, raciest or radical and extremist views.

Contact: being subjected to harmful online interaction with other users, for example commercial advertising as well as adults posing as children or young adults.

Conduct: Personal online behaviour that increases the likelihood of or causes harm, for example making, sending and receiving explicit images, or online bullying.

Within the nursery we aim to keep children, and staff, safe online by:

- Ensuring we have appropriate antivirus and anti-spyware software on all laptops and computers and update them regularly
- Ensuring content blockers and filters are on all our laptops and computers
- Ensuring all devices are password protected and have screen locks. Practitioners are reminded to use complex strong passwords and they are kept safe and secure, changed regularly and not to write them down
- Ensure management monitor all internet activities in the setting
- Locking away all nursery devices at the end of the day
- Ensuring no social media or messaging apps are installed on nursery devices other than the 'Tapestry' tablets which are specifically used for this purpose
- Management reviewing all apps or games downloaded to tablets to ensure all are age appropriate for children and safeguard the children and staff
- Using only nursery devices to record and/or take photographs in the setting
- Never emailing personal or financial information without either using the secure 'Egress' account or first password protecting the documents
- Reporting emails with inappropriate content to the internet watch foundation (IWF www.iwf.org.uk)
- Ensuring children are supervised when using internet devices and that they do not use the 'Tapestry' tablets as these are for adult use only as these contain apps for accessing social media/online content
- Not permitting staff or visitors access to the nursery Wi-Fi on personal devices
- Integrating online safety into nursery daily practice by discussing computer usage 'rules' deciding together what is safe and what is not safe to do online
- Talking to children about 'stranger danger' and deciding who is a stranger and who is not, comparing people in real life situations to online 'friends' e.g. through stories
- When using online video chat, such as Zoom, Teams, Skype, FaceTime etc. (where applicable) discussing with the children what they would do if someone they did not know tried to contact them

- Discussing with the children what they would do if someone they did not know tried to contact them
- Providing training for staff, at least annually, in online safety and understanding how to keep children safe online. We encourage staff and families to complete a free online safety briefing, which can be found at https://moodle.ndna.org.uk/
- Staff modelling safe practice when using technology with children and ensuring all staff abide by an acceptable use policy such as instructing staff to use the nursery IT equipment for matters relating to the children and their education and care only. No personal use will be tolerated (see Acceptable internet use policy)
- Under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material
- Monitoring children's screen time to ensure they remain safe online and have access to material that promotes their development. We will ensure that their screen time is within an acceptable level and is integrated within their programme of learning
- Making sure physical safety of users is considered including the posture of staff and children when using devices
- Being aware of the need to manage our digital reputation, including the appropriateness of information and content that we post online, both professionally and personally. This is continually monitored by the setting's management.
- Ensuring all electronic communications between staff and parents is professional and takes place via the official nursery communication channels, e.g. the setting's email addresses and telephone numbers. This is to protect staff, children and parents.
- Signposting parents to appropriate sources of support regarding online safety at home
- Staff must not friend or communicate with parents on personal devices or social media accounts (please refer to Monitoring Staff Behaviour policy)

If any concerns arise relating to online safety, then we will follow our safeguarding policy and report all online safety concerns to the DSL.

The DSL will make sure that:

- All staff know how to report a problem and when to escalate a concern, including the process for external referral if they feel it is needed

- All concerns are logged, assessed and actioned upon using the Nursery's Safeguarding procedure
- Parents are supported to develop their knowledge of online safety issues concerning their children via the online safety notice board and items in newsletters.
- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern.
- Staff have access to information and guidance for supporting online safety both personally and professionally such as:
- The Professionals Online Safety Helpline (0344 381 4772 or helpline@saferinternet.org.uk) is shared with all staff and used if any concerns arise
- Refer to https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations-for-managers to ensure all requirements are met in order to keep children and staff safe online
- Share https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners with the wider team to help them to keep themselves safe online, both personally and professionally

Cyber Security

This policy should be read in conjunction with our Data protection and Confidentiality Policy, Acceptable IT Use Policy and GDPR Privacy statement.

- Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that Cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity e.g., scam emails. All staff are reminded to follow all the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

- To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.
- Staff are asked to report these to the manager as soon as possible and these will be reported through the NCSC Suspicious Email Reporting Service at report@phishing.gov.uk

This policy was adopted on	**Signed on behalf of the nursery**	**Date for review**
31/05/2023	*J. Hursthouse*	*31/04/2024*